C. Detecting fraudulent modifications
D. Detecting fraudulent disclosure

Correct Answer: D

QUESTION 744
Which of the following is NOT a property of a one-way hash function?

A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.

Correct Answer: A

QUESTION 745
How much more secure is 56 bit encryption opposed to 40 bit encryption?

A. 16 times
B. 256 times
C. 32768 times
D. 65,536 times

Correct Answer: D

QUESTION 746
Which of the following statements is true about data encryption as a method of protecting data?

A. It should sometimes be used for password files.
B. It is usually easily administered.
C. It makes few demands on system resources.
D. It requires careful key Management.

Correct Answer: D

QUESTION 747
The primary purpose for using one-way encryption of user passwords within a system is which of the following?

A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.

B. It prevents an unauthorized person from reading or modifying the password list.
C. It minimizes the amount of storage required for user passwords.
D. It minimizes the amount of processing time used for encrypting password.

Correct Answer: B

QUESTION 748
Which of the following is not a known type of Message Authentication Code (MAC)?

A. Hash function-based MAC
B. Block cipher-based MAC
C. Signature-based MAC
D. Stream cipher-based MAC

Correct Answer: C

QUESTION 749
Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT)?

A. Secure Electronic Transaction (SET)
B. Message Authentication Code (MAC)
C. Cyclic Redundancy Check (CRC)
D. Secure Hash Standard (SHS)

Correct Answer: B

QUESTION 750
Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use a hybrid encryption technique. What does this mean?

A. Use of public key encryption to secure a secret key, and message encryption using the secret key.
B. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
C. Use of software encryption assisted by a hardware encryption accelerator.
D. Use of elliptic curve encryption.

Correct Answer: A

QUESTION 751
One-way hash provides:

A. Confidentiality
B. Availability
C. Integrity
D. Authentication

Correct Answer: C

QUESTION 752
What size is an MD5 message digest (hash)?

A. 128 bits
B. 160 bits
C. 256 bits
D. 128 bytes

Correct Answer: A

QUESTION 753
Which of the following is NOT a property of a one-way hash function?

A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.

Correct Answer: A

QUESTION 754
Which of the following would best describe a Concealment cipher?

A. Permutation is used, meaning that letters are scrambled.
B. Every X number of words within a text, is a part of the real message.
C. Replaces bits, characters, or blocks of characters with different bits, characters, or blocks.
D. Hiding data in another message so that the very existence of the data is concealed.

Correct Answer: B

QUESTION 755
Which of the following ciphers is a subset of the Vigenere polyalphabetic cipher?

A. Caesar
B. Jefferson
C. Alberti
D. SIGABA

Correct Answer: A

QUESTION 756
Which of the following is not a property of the Rijndael block cipher algorithm?

A. Resistance against all known attacks.
B. Design simplicity.
C. 512 bits maximum key size.
D. Code compactness on a wide variety of platforms.

Correct Answer: C

QUESTION 757
What are two types of ciphers?

A. Transposition and Permutation
B. Transposition and Shift
C. Transposition and Substitution
D. Substitution and Replacement

Correct Answer: C

QUESTION 758
Which one of the following, if embedded within the ciphertext, will decrease the likelihood of a message being replayed?

A. Stop bit
B. Checksum
C. Timestamp
D. Digital signature

Correct Answer: C

QUESTION 759
Which of the following statements pertaining to block ciphers is incorrect?

A. It operates on fixed-size blocks of plaintext.
B. It is more suitable for software than hardware implementation.
C. Plain text is encrypted with a public key and decrypted with a private key.
D. Block ciphers can be operated as a stream.

Correct Answer: C

QUESTION 760
The repeated use of the algorithm to encipher a message consisting of many blocks is called

A. Cipher feedback
B. Elliptical curve
C. Cipher block chaining
D. Triple DES

Correct Answer: C

QUESTION 761
When block chaining cryptography is used, what type of code is calculated and appended to the data to ensure authenticity?

A. Message authentication code.
B. Ciphertext authentication code
C. Cyclic redundancy check
D. Electronic digital signature

Correct Answer: A

QUESTION 762
Which of the following statements pertaining to block ciphers is incorrect?

A. It operates on fixed-size blocks of plaintext.
B. It is more suitable for software than hardware implementations.
C. Plain text is encrypted with a public key and decrypted with a private key.
D. Block ciphers can be operated as a stream.

Correct Answer: C